Organizational Information	Response
Organization Name - Combined set of respondents	GENEDGE Alliance - Virginia NIST MEP, Virginia chartered non-profit providing a range of professional services aimed at helping small to medium Virginia businesses grow and prosper. Concurrent Technologies Corporation - non-profit applied research and development professional services organization. Center for Innovative Technology - Virgina chartered not-for-profit with a primary economic development mission on behalf of the Commonwealth of Virginia. Manages the Mach 37 Cyber Security Incubator in Virginia. CMTC - California Manufacturing Technology Consulting is the southern California NIST MEP. CMTC is California's trusted resource for a thriving manufacturing industry. Catalyst Connection - Based in Pittsburgh, Catalyst Connection is a non-profit economic development organization dedicated to helping small manufacturers across southwestern Pennsylvania improve their competitive performance. Catalyst advisors, consultants, and instructors offer training, consulting and administer financial programs that can provide funding for equipment, machinery, or capital improvements.
Organization Sector	All firms are non-profits focused on economic development activities
Organization Size	Ranges from approximately 30 staff to over 800 staff. CTC operates globally. The NIST MEPs operate in their specified states. CIT conducts business globally.
Organization Websites	www.genedge.org www.cit.org www.ctc.com www.cmtc.com www.catalystconnection.org
Point of Contact Information	**Response**
Consortium POC Name	Genedge: Roy Luebke
POC E-mail	rluebke@genedge.org
POC Phone	276-732-8372

#	Question Text	Response Text	References
1	Describe your organization and its interest in the Framework.	GENEDGE is a Commonwealth of Virginia agency and member of the U.S. Department of Commerce/NIST Manufacturing Extension Partnership. Our purpose is to help small businesses growth and prosper in Virginia. We offer a range of services to help small to medium businesses discover new customer opportunities, create new offerings, plan commercialization actions, and provide guidance on LEAN practices to make organizations more effective and competitive. Over the past 2 years, GENEDGE has been meeting with business leaders to learn more about their needs in the area of cyber security. We have discovered that a high percentage of business leaders in smaller businesses do not understand the threats their companies are under from cyber crime. As the Internet of Things begins to explode, small business leaders do not recognize the range of risks their companies are now exposed to as a member of a broad supply chain. Many Virginia-based companies conduct business with the Department of Defense and other federal agencies that are changing the way they will conduct business going forward due to the threats made by cyber criminals. The market price of obtaining quality cyber security protection is very high, often beyond the reach of most smaller companies. GENEDGE has learned that most small business leaders don't understand what the NIST Cyber Framework consists of or why it exists. GENEDGE leadership feels that with extremely high levels of potential loss, we need to bring affordable and high quality cyber risk management to the market. The NIST Cyber Framework can be the roadmap to help business leaders assess their abilities to meet cyber crime challenges and turn them into business opportunities. Our primary interest in the Framework is to use it as the basis for expanding the cyber security capability and resiliency of our manufacturing supply chain.	

#	Question Text	Response Text	References
2	Indicate whether you are responding as a Framework user/non-user, subject matter expert, or whether you represent multiple organizations that are or are not using the Framework.	GENEDGE is the lead for a consortia of MEP centers and private sector providers that is developing subject matter expertise in the use of the Framework. Our objective is to develop a services line for developing company executive and management awareness, capability, risk assessment, risk management plan development, ROI based tool selection and application, and continuous monitoring and updating of the effectiveness of the cyber security risk management plan. GENEDGE and this response represents a consortium of MEPs (PA, IL, Southern CA) along with Virginia's Center for Innovative Technology/Mach 37 Cyber business incubator. GENEDGE is both a user and advisor to other companies about the use and implementation of the Cyber Framework. As a Virginia agency, GENEDGE obtains some IT services via Patrick Henry Community College, and some is provided by our 1-person IT support manager.	
3	If your organization uses the Framework, how do you use it? (e.g., internal management and communications, vendor management, C-suite communication).	GENEDGE has recently begun to review the Framework for applicability to our own business. At this time, we are in the beginning stages of simply assessing our vulnerability points and obtaining external software to provide IT security. GENEDGE is using it internally to pilot the very approach we are looking to provide for our customer base.	

#	Question Text	Response Text	References
4	What has been your organization's experience utilizing specific portions of the Framework (e.g., Core, Profile, Implementation Tiers, Privacy Methodology)?	GENEDGE has not been using the Framework in its security decision making until recently. GENEDGE practices are actually covered within the Framework in the following areas: 1. Identify assets 2. Protect via access control, awareness and staff training, securing corporate data via IBM's. Notes platform, implement Symantec Endpoint protection platform. 3. Performs routine system maintenance, software updates, data backups. 4. Detection of attacks or deterrence of attacks is handled via Symantec's Endpoint platform. Server security is also managed via Patrick Henry Community College's IT department. 5. GENEDGE does have a data recovery plan in place for servers, but not for individual PCs in the field. PC level data management is left to individual staff members.	
5	What portions of the Framework are most useful?	The experience GENEDGE has gained working with clients in Virginia indicates that many small businesses do not understand the extent of the threat that is posed to them in conducting business electronically via the internet. Many business leaders delegate their company's infrastructure security to a very small staff of people, often a single person, to buy some off-the-shelf software and hope that creates enough of a barrier to protect their assets, data, and reputation. Due to that, the risk assessment, management and strategy is of utmost importance. This is the key to understanding how a company should go about protecting both its physical and electronic property. Everything else that the Framework defines is intended to mitigate the risks of conducting business electronically. Our primary interest in the Framework is to use it as the basis for expanding the cyber security capability and resiliency of our manufacturing supply chain. The structure and programmatic steps to improve a company's cyber risk management capability is the most useful aspect of the Framework for our use.	

#	Question Text	Response Text	References
6	What portions of the Framework are least useful?	Our work at GENEDGE indicates that the Recovery section is probably the least used. Not that it isn't useful, but planning for the recovery of something that many people never expect to impact their companies tends to be given little executive attention. However, this area could be of extreme importance at some point in a company's lifecycle. Very little attention appears to be given to on-going communication regarding cyber security, both inside a company and with their supply chain/trading partners. It will be very time consuming for a smaller company to implement the full range of the Framework. Large companies with a large IT staff and more financial resources available will most likely implement a broader range of the Framework.	
7	Has your organization's use of the Framework been limited in any way? If so, what is limiting your use of the Framework (e.g., sector circumstance, organizational factors, Framework features, lack of awareness)?	The GENEDGE experience is that many people don't really understand the purpose and intent of the Framework. They don't really pay any attention to it at all. Especially at the C-level of a business. Even IT people have not heard much about it. In fact, our own IT person has very limited awareness of what it is intended to accomplish.	
8	To what extent do you believe the Framework has helped reduce your cybersecurity risk? Please cite the metrics you use to track such reductions, if any.	For GENEDGE directly, very little impact at this time. For our clients we have not begun to implement yet, but are in the discussion and education and awareness phase. We need to make significant efforts in Virginia to increase awareness and what the Framework can be used to accomplish for a company.	

#	Question Text	Response Text	References
9	What steps should be taken to "prevent duplication of regulatory processes and prevent conflict with or superseding of regulatory requirements, mandatory standards, and related processes" as required by the Cybersecurity Enhancement Act of 2014?	At GENEDGE we are concerned that the U.S. Department of Defense will set up some type of security compliance for any firm wanting to conduct business within DoD. We feel it would be incredibly important for DoD and other federal agencies to work with NIST and make the cyber regulations similar across the entire federal government. Having many different sets of rules will be very costly, time consuming and frustrating to businesses. We suggest that NIST be doing more market awareness events and activities to make people aware of the Framework, and take charge of this issue across the entire federal government. This would then filter out and across industry since federal agencies touch so many varied companies. There are multiple agencies including DoD - NSA - DHS - that are developing voluntary and mandatory guidelines and approaches. It is confusing as to which guidelines, regulations and structure to focus on.	
10	Should the Framework be updated? Why or why not?	GENEDGE suggests that the Framework be a continual work in progress, looking for things that work well and removing elements that do not add any security or business value. To that end, NIST should be executing events around the country to encourage discussion and debate about the various elements and continue to keep the Framework relevant to the changes in the market.	
11	What portions of the Framework (if any) should be changed, or removed? What elements (if any) should be added to the Framework? Please be as specific as possible.	The IPDRR framework is well thought out. It provides a framework for the strategic management of cyber resilience within the company. However, the devices or products which a company produces are not explicitly covered in the framework. This gap should be closed.	

#	Question Text	Response Text	References
12	Are there additions, updates or changes to the Framework's references to cybersecurity standards, guidelines, and practices that should be considered for the update to the Framework?		
13	Are there approaches undertaken by organizations – including those documented in sector-wide implementation guides – that could help other sectors or organizations if they were incorporated into the Framework?	Organizations need to understand that cyber security is as much about risk management as it is technology protection. Many business leaders that we have spoken with look at cyber security as mainly an Information Technology issue. Integrating supply chain management and trading partner relations into the framework would be beneficial. The Carnegie Mellon Capability Maturity Model for systems engineering has some applicability and may be beneficial.	http://cmmiinstitute.com/
14	Should developments made in the nine areas identified by NIST in its Framework-related "Roadmap" be used to inform any updates to the Framework? If so, how?	GENEDGE suggests that serious development work be undertaken in the area of personal authentication and passwords. The existing methods in the market are just not useful for the average person. The use of Smartphones is growing exponentially and will become even more integrated into everyday life. The Internet of Things should be addressed with clarity. Since there are going to be sensors on just about everything in the future, having some structure on how they are used and integrated into systems will be useful. There is a cross over in this to the implementation of Business Continuity Plans, which is heavily promoted by DHS.ccISO 22301 is the reference.	http://www.iso.org/iso/news.htm?refid=Ref1602

#	Question Text	Response Text	References
15	What is the best way to update the Framework while minimizing disruption for those currently using the Framework?	GENEDGE suggests a structure similar to the ISO approach, where the updates are vetted over a period of time with involved participants. Active users would then be prepared to handle updates.	
16	Has information that has been shared by NIST or others affected your use the Framework? If so, please describe briefly what those resources are and what the effect	Information shared by NIST MEP and DHS has been useful. Also information security training from DoD.	
17	What, if anything, is inhibiting the sharing of best practices?	GENEDGE suggests that a common web portal be established and vetted for content by NIST for people to share their findings and uses for the Framework. We are not aware of the existence of such a web-based location at this time. Nothing really inhibits it. However, nothing currently promotes it. There is always a risk in sharing too much to increase the likelihood of a penetrable vulnerability.	
18	What steps could the U.S. government take to increase sharing of best practices?	The government could sponsor regional forums which are sponsored be a multi-agency consortium. The E-3 program which is sponsored by NIST MEP, EPA and DOE is a good example of a working consortia.	

#	Question Text	Response Text	References
19	What kind of program would help increase the likelihood that organizations would share information about their experiences, or the depth and breadth of information sharing (e.g., peer-recognition, trade association, consortia, federal agency)?		
20	What should be the private sector's involvement in the future governance of the Framework?	GENEDGE suggests that private sector companies should have a way to provide information to NIST in a manner that allows NIST to place them into a priorities list of suggested updates. Let many people comment on the proposed updates. When standards are developed and maintained by the private sector, usually the outcome is sustainable. The private sector should ultimately own it and hold itself accountable.	
21	Should NIST consider transitioning some or even all of the Framework's coordination to another organization?	GENEDGE suggests that a non-profit third party could do a fine job of maintaining the framework if properly funded. Take a similar approach as ISO standardization to support a global approach makes sense.	

#	Question Text	Response Text	References
22	If so, what might be transitioned (e.g., all, Core, Profile, Implementation Tiers, Informative References, methodologies)?	All sections should be transitioned to a third-party.	
23	If so, to what kind of organization (e.g., not-for-profit, for-profit; U.S. organization, multinational organization) could it be transitioned, and could it be self-sustaining?	A non-profit would appear to be the most objective way to balance competing thoughts and ideas from a wide variety of sources.	
24	How might any potential transition affect those currently using the Framework? In the event of a transition, what steps might be taken to minimize or prevent disruption for those currently using the Framework?	That can be handled by a coordinated update to the existing ISO standard.	

#	Question Text	Response Text	References
25	What factors should be used to evaluate whether the transition partner (or partners) has the capacity to work closely and effectively with domestic and international organizations and governments, in light of the importance of aligning cybersecurity standards, guidelines, and practices within the United States and globally?	This is a complex question. If the United States considers this to be a somewhat proprietary national security issue, then coordination with ISO has disadvantages. To address this question properly, a rigorous analysis of various approaches would be indicated.	

Question Text	Response Text	References
Describe your organization and its interest in the Framework.	CTC is a non-profit professional services organization. In addition to the insights gained in own implementation of Framework, CTC has partnered with the PA IRC Network to develop a systematic implementation of a customized risk-based assessment methodology aligned and complemented with the NIST Framework for Improving Critical Infrastructure Cybersecurity that can be effectively applied to small to medium size manufacturers.	
Indicate whether you are responding as a Framework user/non-user, subject matter expert, or whether you represent multiple organizations that are or are not using the Framework.	SME	
If your organization uses the Framework, how do you use it? (e.g., internal management and communications, vendor management, C-suite communication).	To complement and validate the cybersecurity assessment approach and to ensure consistent communication of a business's current cybersecurity state and foundational elements for measurement and improvement to decision makers	
What has been your organization's experience utilizing specific portions of the Framework (e.g., Core, Profile, Implementation Tiers, Privacy Methodology)?	We use the framework Core to convey the current cybersecurity state and the Implementation Tiers to measure and convey maturity of processes.	
What portions of the Framework are most useful?	the Core is most relevant and useful	
What portions of the Framework are least useful?	the Privacy Framework had the least direct application for our needs	

Has your organization's use of the Framework been limited in any way? If so, what is limiting your use of the Framework (e.g., sector circumstance, organizational factors, Framework features, lack of awareness)?	Use of the Framework is impeded by corporate lack of awareness of drivers and implementation as it relates to DFARS and other regulatory or contractual requirements. Small businesses in particular may struggle with determining what references directly apply to their environment.	
To what extent do you believe the Framework has helped reduce your cybersecurity risk? Please cite the metrics you use to track such reductions, if any.	The framework Core provides a solid entry point for corporate awareness and a path for risk measurement and continuous improvement.	
What steps should be taken to "prevent duplication of regulatory processes and prevent conflict with or superseding of regulatory requirements, mandatory standards, and related processes" as required by the Cybersecurity Enhancement Act of 2014?	Consistent language and descriptors across all regulatory processes would be a tremendous help and streamline understanding and implementation.	
Should the Framework be updated? Why or why not?	In its current state, the Framework adequately addresses the entire risk management approach and remains adaptable enough that it should only need to be updated when significant change or obsolescence occurs.	
What portions of the Framework (if any) should be changed, or removed? What elements (if any) should be added to the Framework? Please be as specific as possible.	Process and technology aspects are well addressed, but we suggest an additional section on technical resources and how to develop, retain and advance cybersecurity personnel	
Are there additions, updates or changes to the Framework's references to cybersecurity standards, guidelines, and practices that should be considered for the update to the Framework?	Not at this time	

Are there approaches undertaken by organizations – including those documented in sector-wide implementation guides – that could help other sectors or organizations if they were incorporated into the Framework?	No, the framework should not try to be one size fits all - sector-specific guidance should drive effective framework implementation.	
Should developments made in the nine areas identified by NIST in its Framework-related "Roadmap" be used to inform any updates to the Framework? If so, how?	If a roadmap has been created to provide a path forward then yes, significant developments made in those nine areas should be reflected in future updates.	
What is the best way to update the Framework while minimizing disruption for those currently using the Framework?	Socialization of anticipated Framework updates well in advance should minimize disruption and support planning and decision making for current users.	
Has information that has been shared by NIST or others affected your use the Framework? If so, please describe briefly what those resources are and what the effect has been on your use of the Framework. What resources, if any, have been most useful?	NA	
What, if anything, is inhibiting the sharing of best practices?	The maturity of trusted communication and information sharing networks focused on specific sectors is still a gap.	
What steps could the U.S. government take to increase sharing of best practices?	Provide funding and incentives to existing industry networks in critical infrastructure sectors, with a focus on implementation (beyond awareness and training). Networks should include both users and solution providers.	

What kind of program would help increase the likelihood that organizations would share information about their experiences, or the depth and breadth of information sharing (e.g., peer-recognition, trade association, consortia, federal agency)?	A “neighborhood watch” approach to cybersecurity would allow companies to build information networks based on trust, share mitigation and remediation strategies, to gain specific threat intelligence.	
What should be the private sector’s involvement in the future governance of the Framework?	Continue to provide feedback and boundaries.	
Should NIST consider transitioning some or even all of the Framework’s coordination to another organization?	It would seem that NIST is in the best position to maintain the Core but the Implementation Tiers could be transitioned to a neutral third party.	
If so, what might be transitioned (e.g., all, Core, Profile, Implementation Tiers, Informative References, methodologies)?	Implementation Tiers	
If so, to what kind of organization (e.g., not-for-profit, for-profit; U.S. organization, multinational organization) could it be transitioned, and could it be self-sustaining?	Transition to a not-for profit technical organization that is solution agnostic could be considered. The feasibility of that entity becoming fully self-sustaining may be unacheivable and perhaps unadvisable.	
How might any potential transition affect those currently using the Framework? In the event of a transition, what steps might be taken to minimize or prevent disruption for those currently using the Framework?		

What factors should be used to evaluate whether the transition partner (or partners) has the capacity to work closely and effectively with domestic and international organizations and governments, in light of the importance of aligning cybersecurity standards, guidelines, and practices within the United States and globally?		

#	Question Text	Response Text	References
1	Describe your organization and its interest in the Framework.	CIT is a State chartered not-for-profit with a primary economic development mission on behalf of the Commonwealth of Virginia. Our primary focus is on early stage companies in high growth sectors, and our programs offer a range of support for early stage companies, including opportunities to participate in our Cybersecurity accelerator, Mach37, as well as opportunities for direct grants or equity investments.	
2	Indicate whether you are responding as a Framework user/non-user, subject matter expert, or whether you represent multiple organizations that are or are not using the Framework.	CIT uses the framework directly in our internal operations as well as using the framework for guidance with the third-party businesses we interact with.	

3	If your organization uses the Framework, how do you use it? (e.g., internal management and communications, vendor management, C-suite communication).	We use the framework for guidance within 3 IT governance structures. 1) As an Authority within the Virginia IT Agency (VITA) umbrella, we are subject to VITA-dictated policy and governance, which uses the framework as one of their guidance documents in formulating the State policies captured in SEC-501. 2) as a stand-alone entity, CIT uses the framework directly as guidance for the strategic development of our own cybersecurity posture for networks we control. 3) as an investor and mentor organization for many small companies, we use the framework increasingly to help assess the security posture of the early stage companies we interact with	
4	What has been your organization's experience utilizing specific portions of the Framework (e.g., Core, Profile, Implementation Tiers, Privacy Methodology)?	The Core has been a great help in organizing our thinking around cybersecurity and being able to communicate effectively with both internal and external stakeholders. The notions of implementation tiers and profiles is useful at a conceptual level but not much help at an implementation level.	
5	What portions of the Framework are most useful?	Core	
6	What portions of the Framework are least useful?	Notion of profile is great; actual construction of profiles is an exercise left mostly to the reader	

7	Has your organization's use of the Framework been limited in any way? If so, what is limiting your use of the Framework (e.g., sector circumstance, organizational factors, Framework features, lack of awareness)?	Yes. Once initial status is determined, particularly as a small business, the ability to sort through commercial offerings, determine their value, and prioritize the ones that are affordable is the limiting factor.	
8	To what extent do you believe the Framework has helped reduce your cybersecurity risk? Please cite the metrics you use to track such reductions, if any.	Modestly. Initially the framework has helped move us to implement more active and continuous network monitoring, and to that extent our risk has been reduced. We use a tool that numerically scores risk, and the frequency of risk scores above certain thresholds is the primary metric.	
9	What steps should be taken to "prevent duplication of regulatory processes and prevent conflict with or superseding of regulatory requirements, mandatory standards, and related processes" as required by the Cybersecurity Enhancement Act of 2014?	Keep the framework voluntary	

10	Should the Framework be updated? Why or why not?	No, or only modest tweaks. The cultural change of getting people to accept such a framework is finally starting to gain some traction, and significant structural changes would both create confusion and diminish the more common understanding about cybersecurity that is beginning to emerge	
11	What portions of the Framework (if any) should be changed, or removed? What elements (if any) should be added to the Framework? Please be as specific as possible.		
12	Are there additions, updates or changes to the Framework's references to cybersecurity standards, guidelines, and practices that should be considered for the update to the Framework?		

13	Are there approaches undertaken by organizations – including those documented in sector-wide implementation guides – that could help other sectors or organizations if they were incorporated into the Framework?	Trying to cram everything into a single framework instead of keeping it simple is a path to disaster. Work with other sector groups to have them take the lead on extending the framework to those communities of interest. This probably applies to information-sharing as well.	
14	Should developments made in the nine areas identified by NIST in its Framework-related "Roadmap" be used to inform any updates to the Framework? If so, how?	The nine roadmap areas ARE areas where it makes sense to work with non-Governmental partners, since there is a lot of commercial activity already ongoing in these areas and bringing them into alignment with the current framework would be helpful. For example, Supply Chain Risk Management is one identified area, and the NIST MEP structure is actively working to apply the framework in this domain since it is their area of expertise. NIST funding for these types of efforts to supplement the existing framework could have large positive effects in actual implementation of best practices across a larger set of industry players.	
15	What is the best way to update the Framework while minimizing disruption for those currently using the Framework?	Leave the core alone, and build supporting documents or standards around it.	

16	Has information that has been shared by NIST or others affected your use the Framework? If so, please describe briefly what those resources are and what the effect has been on your use of the Framework. What resources, if any, have been most useful?	References to framework and supporting standards by public speakers from NIST or other Government organizations help provide interpretation of the framework and how it fits into the larger scheme of things	
17	What, if anything, is inhibiting the sharing of best practices?	Industry groups are already sharing best practices. Efforts by some to initiate cross-sector groups suffer from two issues: overload of CISOs who would actually do the sharing to participate in yet another activity, and lack of incentives to share due to asymmetry of these groups...lots of lurkers and few contributors. Also, relatively few organizations have the wherewithal to follow through even when sharing is good	
18	What steps could the U.S. government take to increase sharing of best practices?	Provide Safe Harbor without simultaneously trying to diminish perceptions of reduction in privacy protections	

19	What kind of program would help increase the likelihood that organizations would share information about their experiences, or the depth and breadth of information sharing (e.g., peer-recognition, trade association, consortia, federal	A robust cyber insurance market that has premium reductions for good cyber behaviors, including participation in information sharing groups	
20	What should be the private sector's involvement in the future governance of the Framework?	Private sector standards bodies tend to get "owned" by a small group of participants with their own interests at heart rather than the broader industry or public. Keep it at NIST.	
21	Should NIST consider transitioning some or even all of the Framework's coordination to another organization?	No	
22	If so, what might be transitioned (e.g., all, Core, Profile, Implementation Tiers, Informative References, methodologies)?		

23	If so, to what kind of organization (e.g., not-for-profit, for-profit; U.S. organization, multinational organization) could it be transitioned, and could it be self-sustaining?	If done, not-for-profit. No obvious business model for making this self-sustaining	
24	How might any potential transition affect those currently using the Framework? In the event of a transition, what steps might be taken to minimize or prevent disruption for those currently using the Framework?	One of two things…either people would start dis-regarding the standard after public transition or else new owners try to enforce it as a standard, which reduces the value of the framework, now voluntary	

25	What factors should be used to evaluate whether the transition partner (or partners) has the capacity to work closely and effectively with domestic and international organizations and governments, in light of the importance of aligning cybersecurity standards, guidelines, and practices within the United States and globally?		

#	Question Text	Response Text	References
1	Describe your organization and its interest in the Framework.	CMTC is the MEP for Southern California with an interest in adapting the NIST Cybersecurity Framework to make it an actionable tool for use by SMMs in California.	
2	Indicate whether you are responding as a Framework user/non-user, subject matter expert, or whether you represent multiple organizations that are or are not using the Framework.	CMTC has plans to use the framework and is in discussion with a large OEM that has an interest in using the framework throughout their extended supply chain. Additionally, CMTC is working with a number of national labs and California universities to understand how these organizations use the framework in order to capture best practices to transfer to SMMs.	
3	If your organization uses the Framework, how do you use it? (e.g., internal management and communications, vendor management, C-suite communication).	Currently CMTC uses the framework for C-Suite communication with plans to eventually use it for vendor management.	
4	What has been your organization's experience utilizing specific portions of the Framework (e.g., Core, Profile, Implementation Tiers, Privacy Methodology)?	CMTC is currently examining how a leading OEM is using the Core and risk profile portions.	
5	What portions of the Framework are most useful?	Too early to tell.	

6	What portions of the Framework are least useful?	Too early to tell.	
7	Has your organization's use of the Framework been limited in any way? If so, what is limiting your use of the Framework (e.g., sector circumstance, organizational factors, Framework features, lack of awareness)?	CMTC is working to traverse the learning curve regarding the framework. CMTC has also encountered lack of awareness and understanding of the framework.	
8	To what extent do you believe the Framework has helped reduce your cybersecurity risk? Please cite the metrics you use to track such reductions, if any.	Too early to tell.	
9	What steps should be taken to "prevent duplication of regulatory processes and prevent conflict with or superseding of regulatory requirements, mandatory standards, and related processes" as required by the Cybersecurity Enhancement Act of 2014?	N/A	
10	Should the Framework be updated? Why or why not?	CMTC's experience is that the Framework is comprehensive enough to provide significant value. Development of awareness of the framework and tools to facilitate the use of the framework would be a valuable next step	

11	What portions of the Framework (if any) should be changed, or removed? What elements (if any) should be added to the Framework? Please be as specific as possible.	CMTC's perspective is that the framework does not currently need specific revision. However, taking the framework and tailoring the content to various stakeholder roles (CEO, CTO, IT Director, etc.) would be of benefit	
12	Are there additions, updates or changes to the Framework's references to cybersecurity standards, guidelines, and practices that should be considered for the update to the Framework?	The framework currently appears to be comprehensive, however a periodic review of the framework to revise or upgrade due to advances in IoT, augmented reality and the data analytics to support artificial intelligence seem warranted	
13	Are there approaches undertaken by organizations – including those documented in sector-wide implementation guides – that could help other sectors or organizations if they were incorporated into the Framework?	Too early to tell.	
14	Should developments made in the nine areas identified by NIST in its Framework-related "Roadmap" be used to inform any updates to the Framework? If so, how?	Yes, from an OEM perspective, how does the OEM use the framework to roll cybersecurity best practices down the tiers of their supplier network? From the SMM perspective, how does the SMM systematically implement the framework?	

15	What is the best way to update the Framework while minimizing disruption for those currently using the Framework?	In the short and intermediate term, perhaps it is best to not change the framework, but instead focus on making it easier to understand and incrementally implement. The framework is valuable as is, and while maybe not perfect, can help get industry on the road to higher security.	
16	Has information that has been shared by NIST or others affected your use the Framework? If so, please describe briefly what those resources are and what the effect has been on your use of the Framework. What resources, if any, have been most useful?	CMTC's experience has been limited to the framework itself, not to other information or materials or resources.	
17	What, if anything, is inhibiting the sharing of best practices?	Lack of awareness of cybersecurity risks; competitive pressure; siloes within an organization	
18	What steps could the U.S. government take to increase sharing of best practices?	Replicate best practices from ICS CERT and InfraGard to benefit SMMs	

19	What kind of program would help increase the likelihood that organizations would share information about their experiences, or the depth and breadth of information sharing (e.g., peer-recognition, trade association, consortia, federal agency)?	Due to the sensitive nature and negative effects on business reputations and results of security breaches, perhaps a program that allows for the anonymous sharing of breach information, scope and general effects would be in order. Taking this to another level, a gaming program could be a powerful tool to raise awareness of security vulnerabilities, fostering participation by subject matter experts, and providing platforms for sharing, understanding and preventing cybersecurity breaches.	
20	What should be the private sector's involvement in the future governance of the Framework?	The private sector should have a significant role in governance, with a strong bias toward SMM's over large companies.	
21	Should NIST consider transitioning some or even all of the Framework's coordination to another organization?	No	
22	If so, what might be transitioned (e.g., all, Core, Profile, Implementation Tiers, Informative References, methodologies)?	N/A - the framework should not be changed	
23	If so, to what kind of organization (e.g., not-for-profit, for-profit; U.S. organization, multinational organization) could it be transitioned, and could it be self-sustaining?	N/A - the framework should not be changed	

24	How might any potential transition affect those currently using the Framework? In the event of a transition, what steps might be taken to minimize or prevent disruption for those currently using the Framework?	N/A - the framework should not be changed	
25	What factors should be used to evaluate whether the transition partner (or partners) has the capacity to work closely and effectively with domestic and international organizations and governments, in light of the importance of aligning cybersecurity standards, guidelines, and practices within the United States and globally?	N/A - the framework should not be changed	